Question Paper Code: U9278

B.E./B.Tech. DEGREE EXAMINATION, APRIL 2024

Open Elective

21UCS978 NETWORK SECURITY ESSENTIALS

(Common to ALL branches)

(Regulations 2021)

Duration: Three hours   Maximum: 100 Marks

Answer ALL Questions

PART A - (10 x 2 = 20 Marks)

1.	Define network security.	CO1 - U
2.	Define categories of security services.	CO1 - U
3.	Convert the given Text "VALLIAMMAI" into cipher text using Rail fence Technique.	CO2-App
4.	Perform encryption and decryption using RSA algorithm for the following. p=7, q=11; e=17; m=8.	CO2-App
5.	Define distribution system a wireless network.	CO1 - U
6.	What services are provided by WSP?	CO1 - U
7.	Why E-mail compatibility function in PGP needed?	CO1 - U
8.	What is a replay attack?	CO1 - U
9.	Describe some countermeasures against worms.	CO1 - U
10.	What is a digital immune system?	CO1 - U

PART – B (5 x 16= 80 Marks)

11. (a) Explain Data Encryption Standard (DES) in detail. How AES is used for encryption/decryption? Discuss with example?   CO1 - U   (16)

Or

(b) Explain the key management of public key encryption in detail?   CO1 - U   (16)

12. (a) Encrypt the following using play fair cipher using the keyword MONARCHY. Use X for blank spaces "SWARAJ IS MY BIRTH RIGHT"   CO2-App   (16)

Or

(b) Write the Extended Euclidean algorithm to solve gcd (98, 56).   CO2-App   (16)

13. (a) State and prove the Chinese remainder theorem. What are the last two digits of 4919? CO2-App (16)

Or

(b) Examine Elliptic Curve Cryptography to simulate ElGamal algorithm. CO2-App (16)

14. (a) Explain the architecture of IPsec in detail in detail with a neat block diagram CO1 - U (16)

Or

(b) Describe PGP cryptographic functions in detail with suitable block diagrams. CO1 - U (16)

15. (a) Analyze the different types of virus in detail. Suggest scenarios for deploying these types in network scenario CO1 - U (16)

Or

(b) Explain intrusion detection system (IDS) in detail with suitable diagram CO1 - U (16)

U9278